Real-Time Vulnerability Management

Operationalizing the VM process from detection to remediation

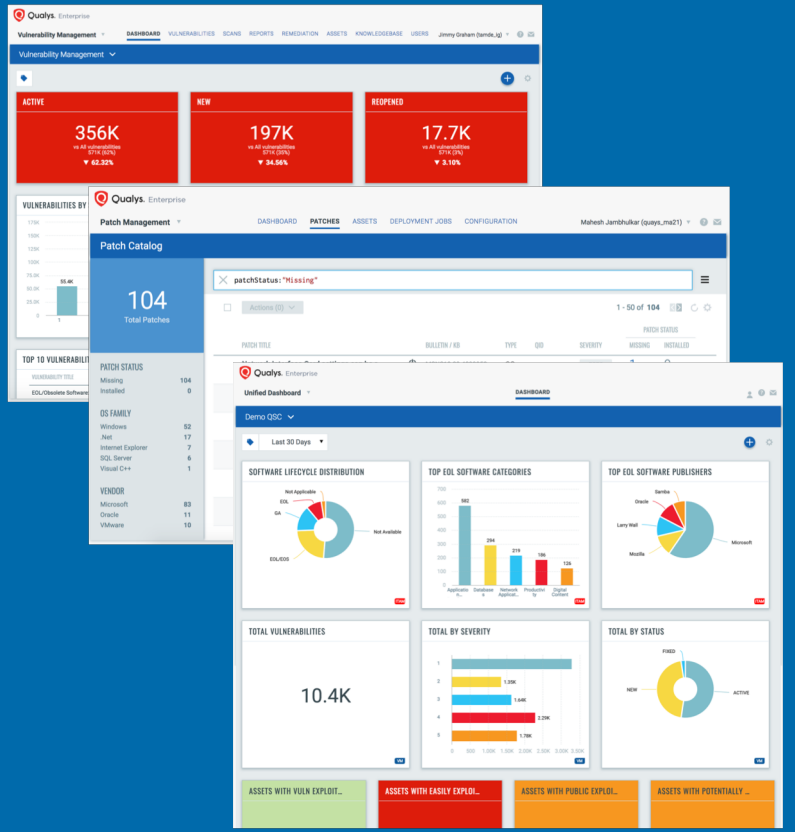
Jimmy Graham
Senior Director, Product Management, Qualys, Inc.

Agenda

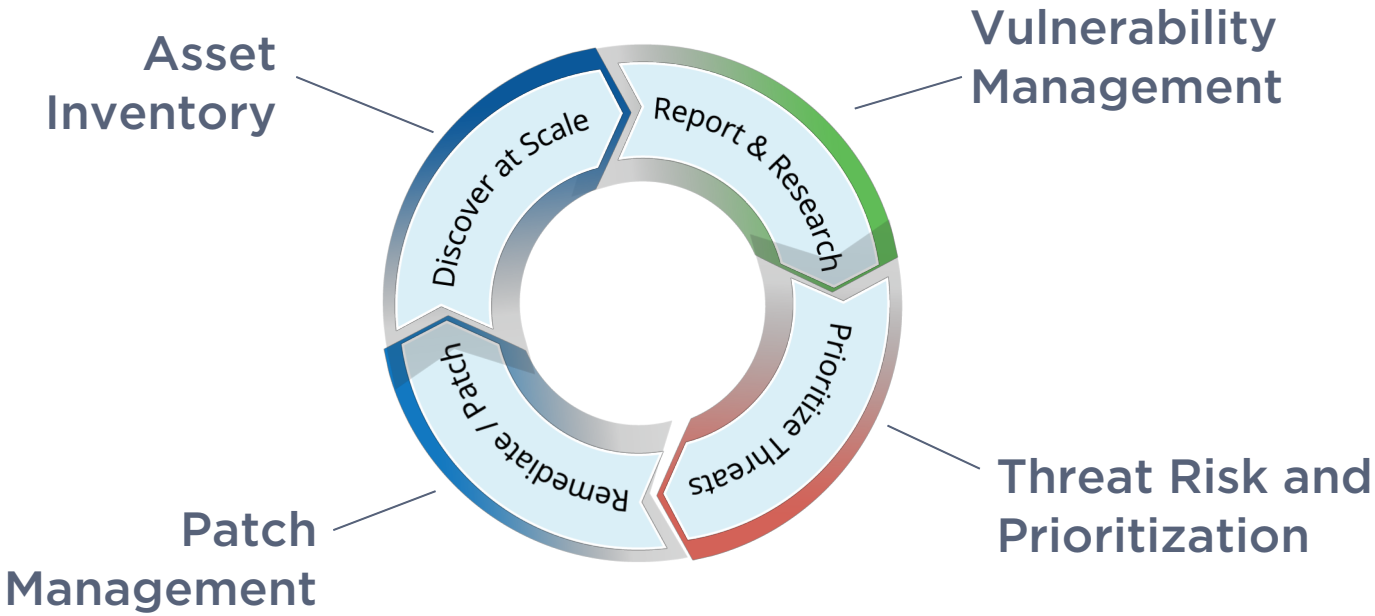
Expanding Vulnerability Management

Vulnerability Management Platform Evolution

Introducing Qualys Patch Management



Vulnerability Management Lifecycle

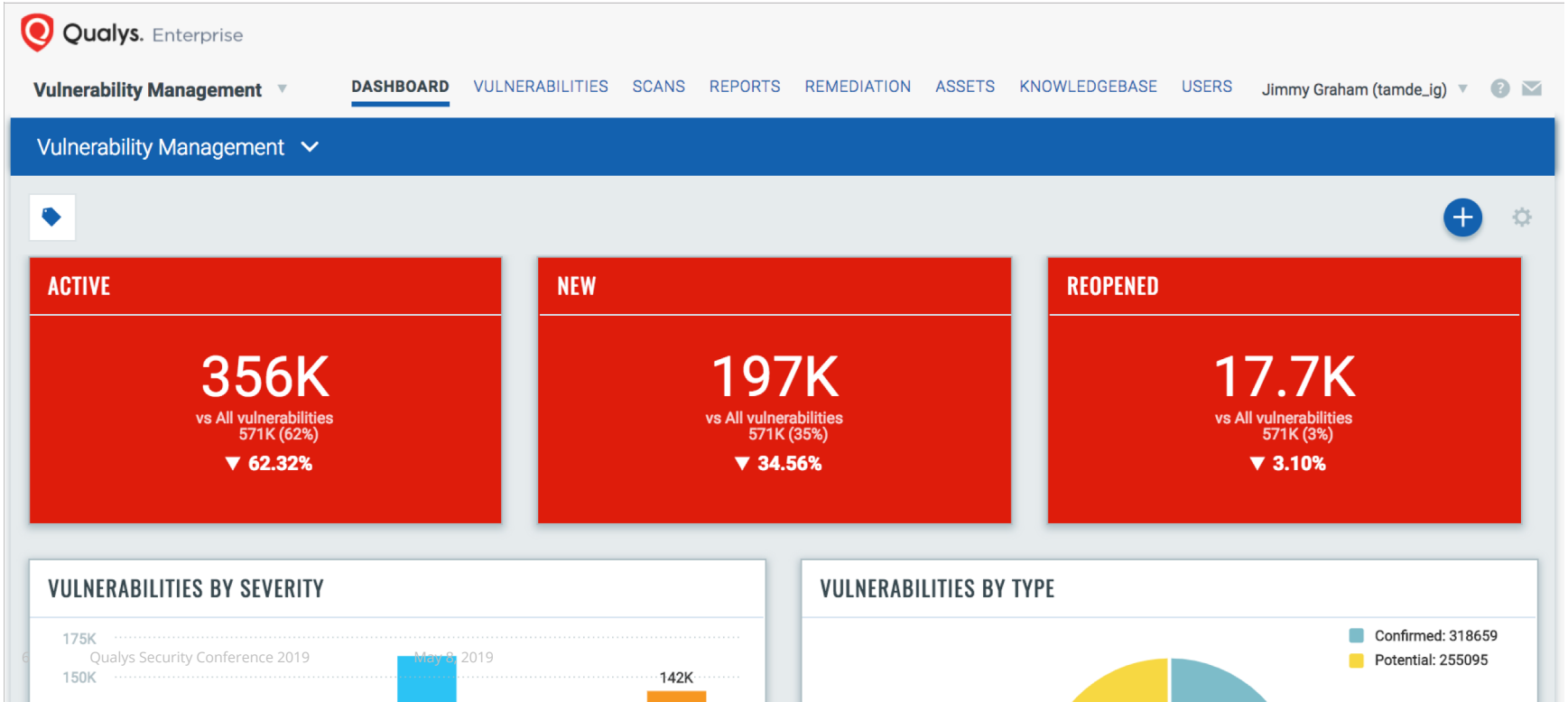


Expanding Vulnerability Management

Qualys.

Vulnerability Management

Platform Evolution



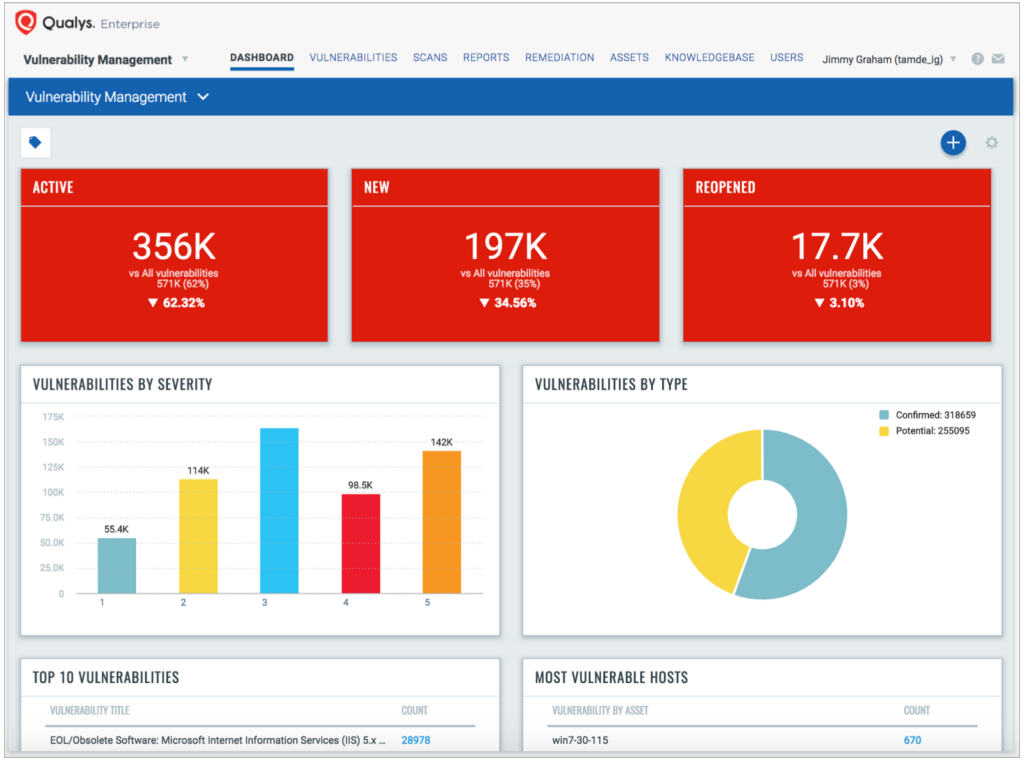
Dynamic VM Dashboard

Merges AssetView technology into Qualys VM

Build widgets with vulnerability counts

Search filters for quickly building queries

Replace long-running reports with live widgets



Qualys.

Opening Up the VM Detections Platform

Custom Remote Detections

Qualys Remote Detection Interface (QRDI)

Create your own or share on Qualys Community

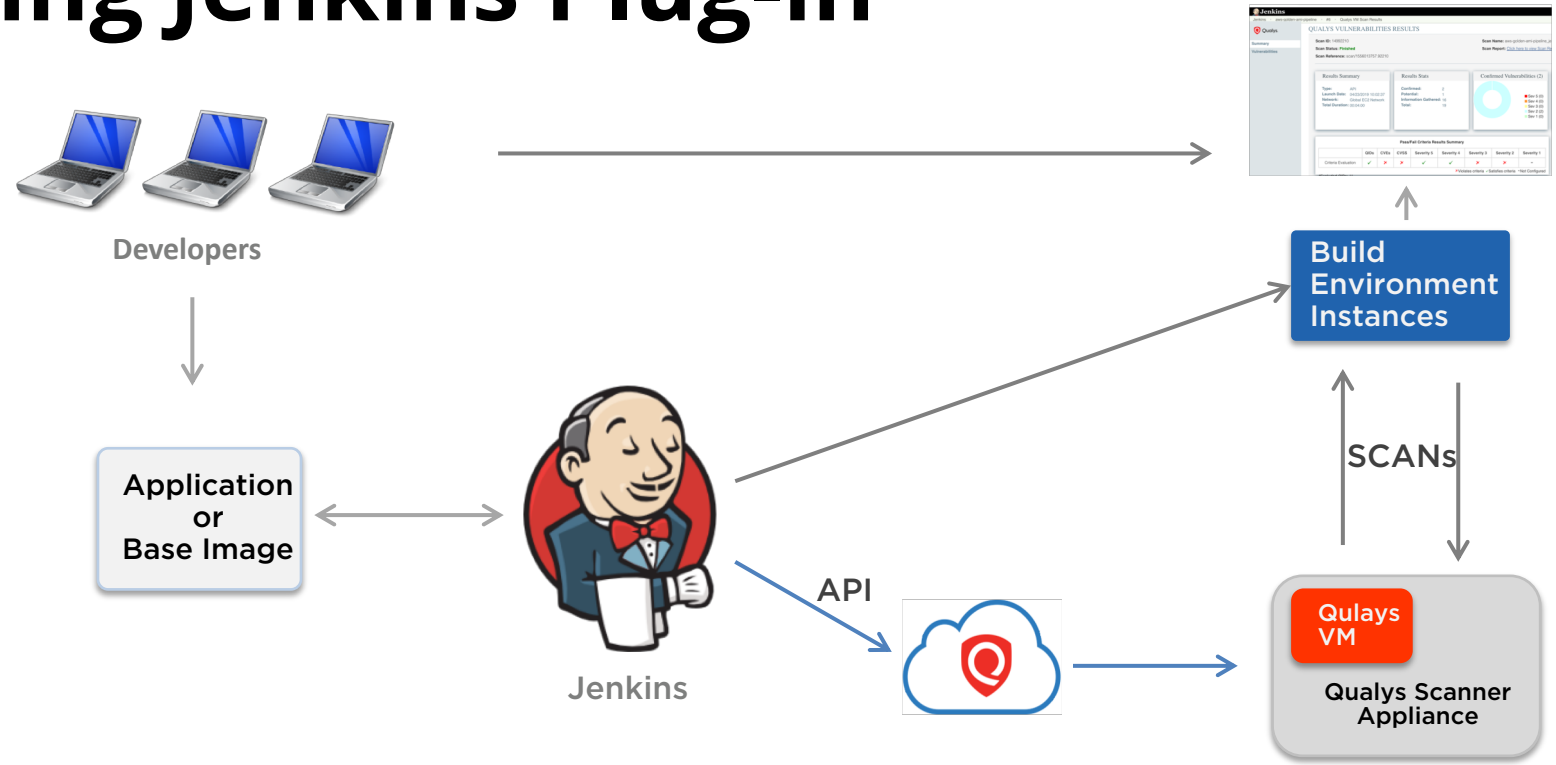
Supports HTTP(S) and raw TCP

Regex grouping and capturing

LUA scripting for advanced logic

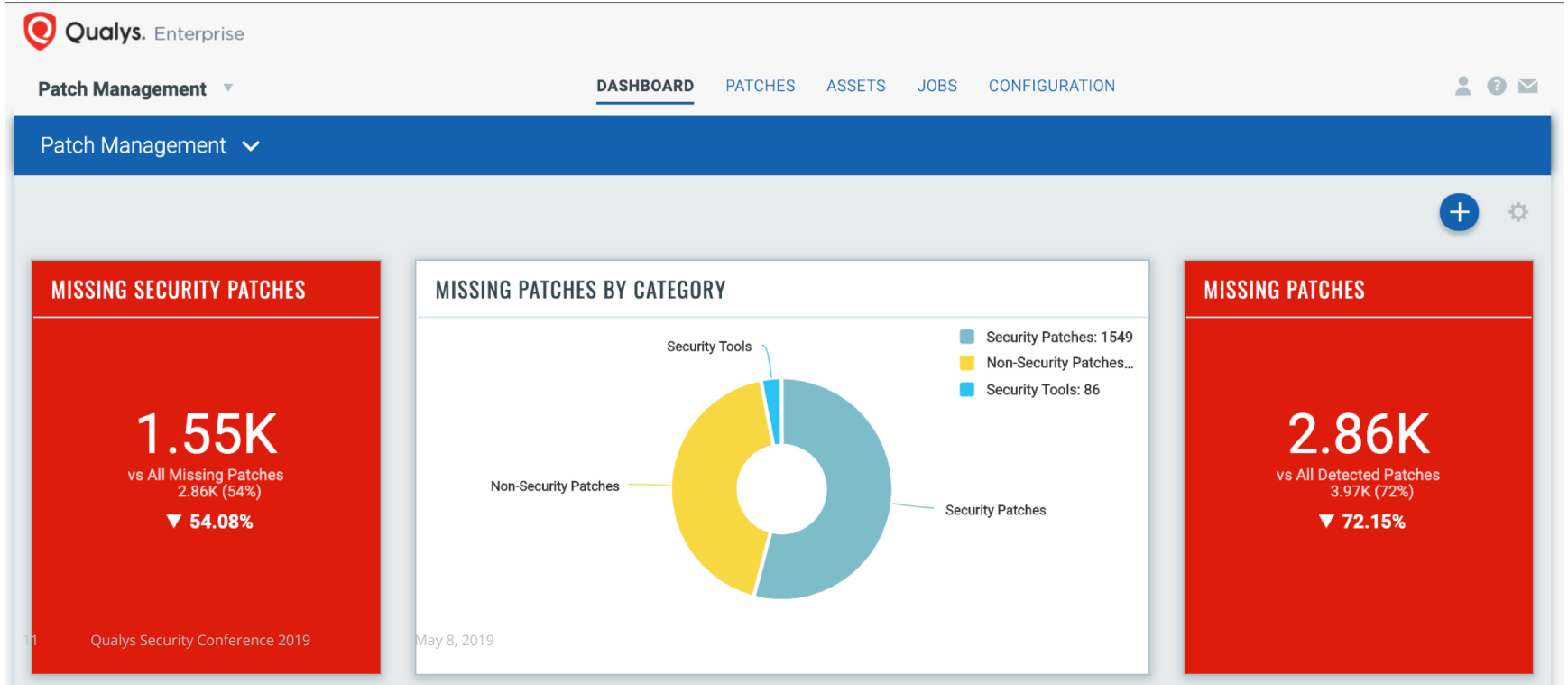
Qualys.

Qualys Vulnerability Assessment using Jenkins Plug-in



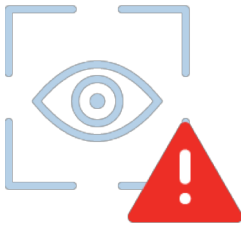
Qualys Patch Management

Overview



Current Patch Management Tools

Challenges and Impact



Manual correlation of vulnerability to patch leads to delayed mean-time-to-remediation

Waiting for vulnerability reports to confirm remediation

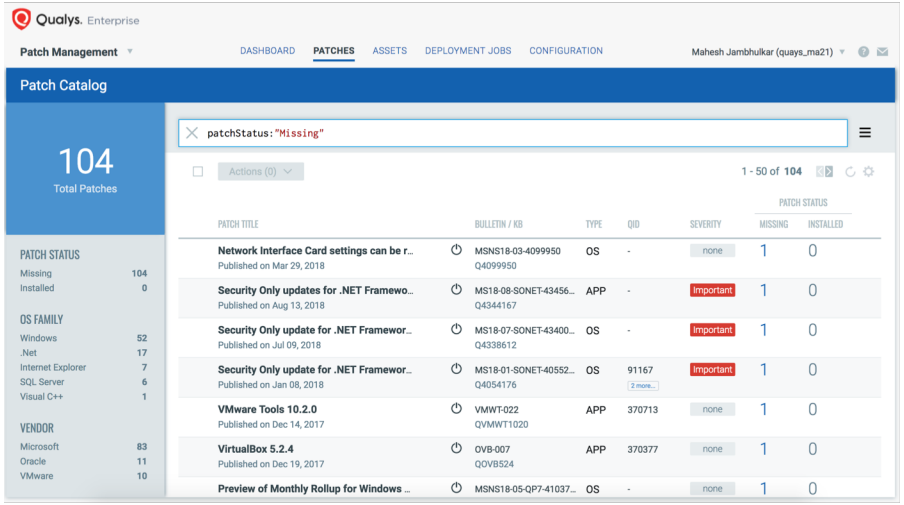
Remote systems only patched when connected to corporate network

Limited or no coverage of third-party apps

Multiple patching solutions for each OS type

Introducing

Qualys Patch Management



- Automated correlation of vulnerability and patch data – Which patch fixes the CVE?
- Simple dashboarding for tracking missing patches
- Patch using the Qualys Cloud Agent, anywhere
- Patch OS and third-party applications
- Single solution for Windows, macOS, and Linux

DEMO

Patch Management

Platform Support

XP SP3+

Vista

Windows 7

Windows 8/8.1

Windows 10

Server 2003 SP2+

Server 2008/R2

Server 2012/R2

Server 2016

Server 2019

OS X 10.10
Yosemite

OS X 10.11
El Capitan

macOS 10.12
Sierra

macOS 10.13
High Sierra

macOS 10.14
Mojave

RHEL 6,7

CentOS 5.4+,6,7

SUSE Linux Enterprise
Server/ Desktop
11,12,15

Oracle Ent Linux
6,7(Server)

Ubuntu
14.x,15.x,16.x,18.x

* Roadmap items are future-looking; timing and specifications may change

Qualys.

Patch Management Roadmap

Patch Management 1.0

March 2019

Windows patching (desktops and servers)

Qualys serves patches

Third party Windows applications

Patch Management 1.2

May 2019

On-prem Caching of patches (CAG)

Direct download from vendors for off-prem

Tag-based user scoping

Patch Management 1.3+

Mac patching

Linux patching w/

Repository integration

Role-based access control

Automation Rules & Approval workflows

Qualys.

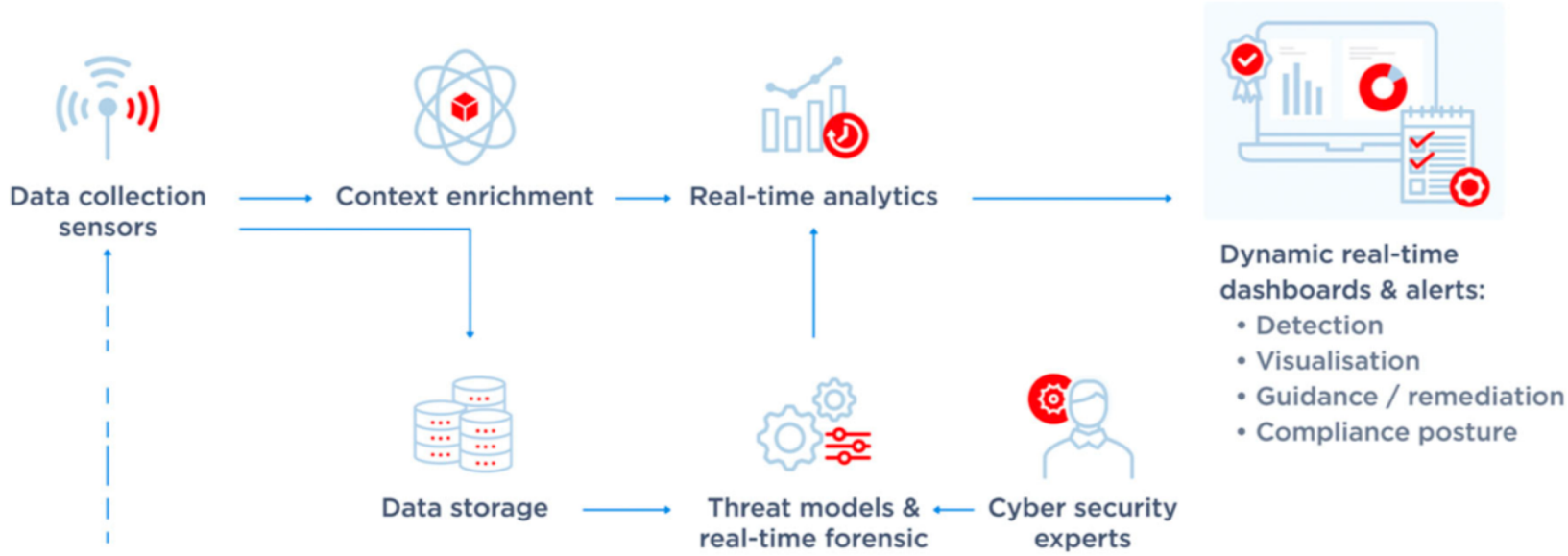
Thank You

Jimmy Graham
jgraham@qualys.com

Transform Valuable Insights into Actionable Data-Driven Decisions

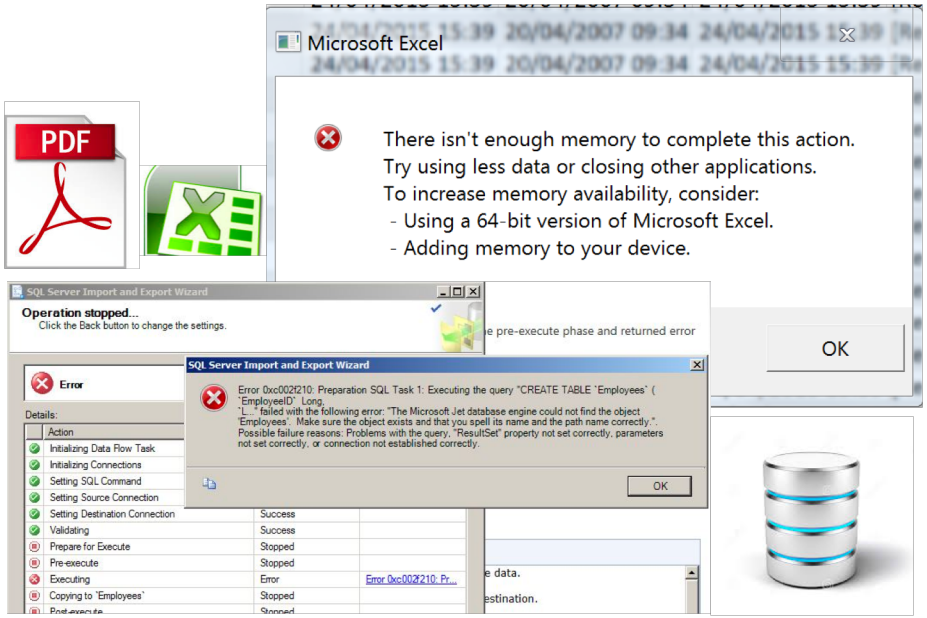
Felix Jimenez
Director of Product Management Qualys, Inc.

Turning Data Into Insights



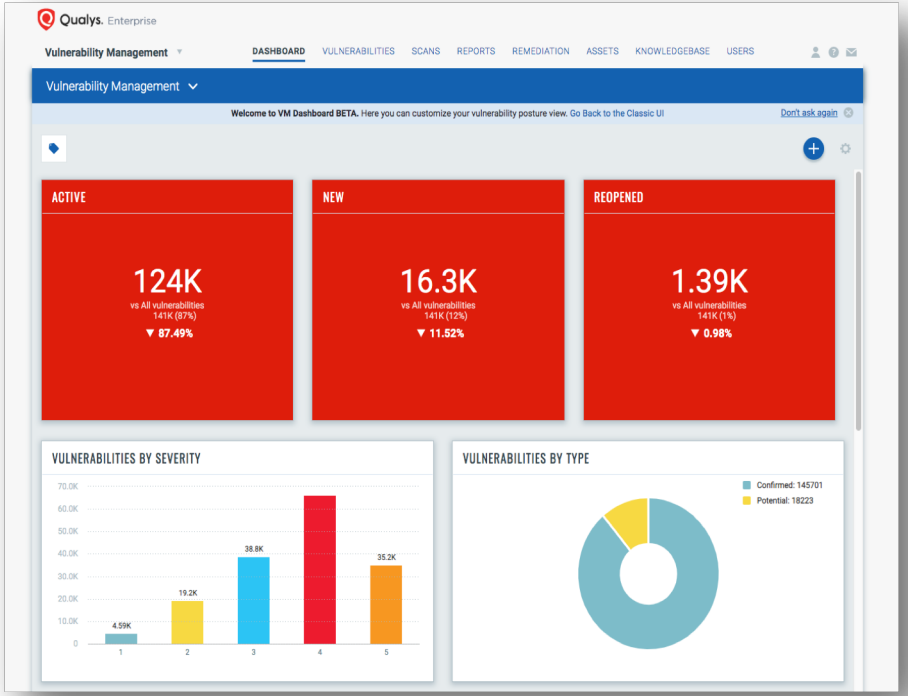
Qualys.

Problems of Manual Data Visualizations


Microsoft Excel
There isn't enough memory to complete this action.
Try using less data or closing other applications.
To increase memory availability, consider:
- Using a 64-bit version of Microsoft Excel.
- Adding memory to your device.
OK
SQL Server Import and Export Wizard
Operation stopped...
Click the Back button to change the settings.
SQL Server Import and Export Wizard
Error 0xc002f210: Preparation SQL Task 1: Executing the query "CREATE TABLE 'Employees' ('EmployeeID' Long, 'L..." failed with the following error: "The Microsoft Jet database engine could not find the object 'Employees'. Make sure the object exists and that you spell its name and the path name correctly.". Possible failure reasons: Problems with the query, "ResultSet" property not set correctly, parameters not set correctly, or connection not established correctly.
OK
Error
Details:
Action
Initializing Data Flow Task
Initializing Connections
Setting SQL Command
Setting Source Connection
Setting Destination Connection
Validating
Prepare for Execute
Pre-execute
Executing
Copying to 'Employees'
Success
Success
Stopped
Stopped
Error
Stopped

- Too many dependencies
- Time consuming
- Not Actionable
- No Context
- Static
- Doesn't allow you to adjust focus

Actionable Dashboarding

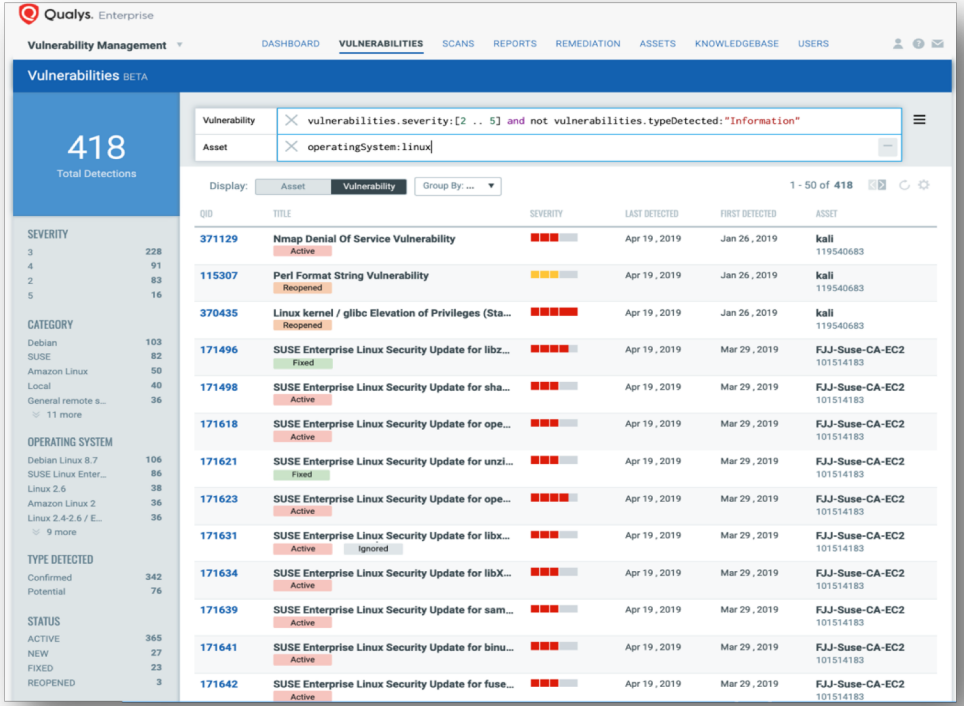


Dashboards powered by Qualys Query Language (QQL).

Enables a comprehensive, and customizable, simple view of your risk landscape based upon the constant feed of data available in your subscription.

GA – June 2019

Faceted Search Queries


Qualys. Enterprise
Vulnerability Management
DASHBOARD
VULNERABILITIES
SCANS
REPORTS
REMEDIATION
ASSETS
KNOWLEDGEBASE
USERS
Vulnerabilities BETA
418
Total Detections
Vulnerability
vulnerabilities.severity:[2 .. 5] and not vulnerabilities.typeDetected:"Information"
Asset
operatingSystem:linux
Display:
Asset
Vulnerability
Group By: ...
1 - 50 of 418
QID
TITLE
SEVERITY
LAST DETECTED
FIRST DETECTED
ASSET
371129 Nmap Denial Of Service Vulnerability Active Apr 19, 2019 Jan 26, 2019 kali 119540683
115307 Perl Format String Vulnerability Reopened Apr 19, 2019 Jan 26, 2019 kali 119540683
370435 Linux kernel / glibc Elevation of Privileges (Sta... Reopened Apr 19, 2019 Jan 26, 2019 kali 119540683
171496 SUSE Enterprise Linux Security Update for libz... Fixed Apr 19, 2019 Mar 29, 2019 FJJ-Suse-CA-EC2 101514183
171498 SUSE Enterprise Linux Security Update for sha... Active Apr 19, 2019 Mar 29, 2019 FJJ-Suse-CA-EC2 101514183
171618 SUSE Enterprise Linux Security Update for ope... Active Apr 19, 2019 Mar 29, 2019 FJJ-Suse-CA-EC2 101514183
171621 SUSE Enterprise Linux Security Update for unzi... Fixed Apr 19, 2019 Mar 29, 2019 FJJ-Suse-CA-EC2 101514183
171623 SUSE Enterprise Linux Security Update for ope... Active Apr 19, 2019 Mar 29, 2019 FJJ-Suse-CA-EC2 101514183
171631 SUSE Enterprise Linux Security Update for libx... Active Ignored Apr 19, 2019 Mar 29, 2019 FJJ-Suse-CA-EC2 101514183
171634 SUSE Enterprise Linux Security Update for libX... Active Apr 19, 2019 Mar 29, 2019 FJJ-Suse-CA-EC2 101514183
171639 SUSE Enterprise Linux Security Update for sam... Active Apr 19, 2019 Mar 29, 2019 FJJ-Suse-CA-EC2 101514183
171641 SUSE Enterprise Linux Security Update for binu... Active Apr 19, 2019 Mar 29, 2019 FJJ-Suse-CA-EC2 101514183
171642 SUSE Enterprise Linux Security Update for fuse... Active Apr 19, 2019 Mar 29, 2019 FJJ-Suse-CA-EC2 101514183
SEVERITY
3 228
4 91
2 83
5 16
CATEGORY
Debian 103
SUSE 82
Amazon Linux 50
Local 40
General remote s... 36
11 more
OPERATING SYSTEM
Debian Linux 8.7 106
SUSE Linux Enter... 86
Linux 2.6 38
Amazon Linux 2 36
Linux 2.4-2.6 / E... 36
9 more
TYPE DETECTED
Confirmed 342
Potential 76
STATUS
ACTIVE 365
NEW 27
FIXED 23
REOPENED 3

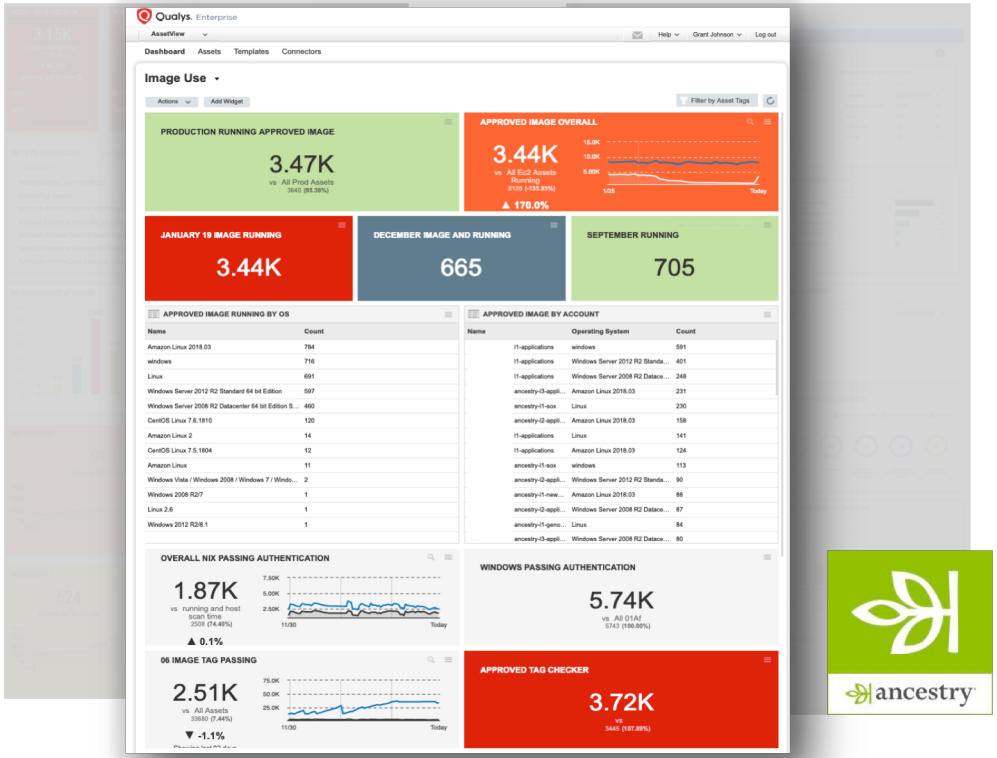
Single page when viewing asset or vulnerability information.

Quick Vulnerability Status.

Vulnerability age.

Group by different data points

Turn Data into Insights



It's not enough to know that an Cloud instance exists.

Where does it live?

What OS is it running?

What software is installed and at what patch level?

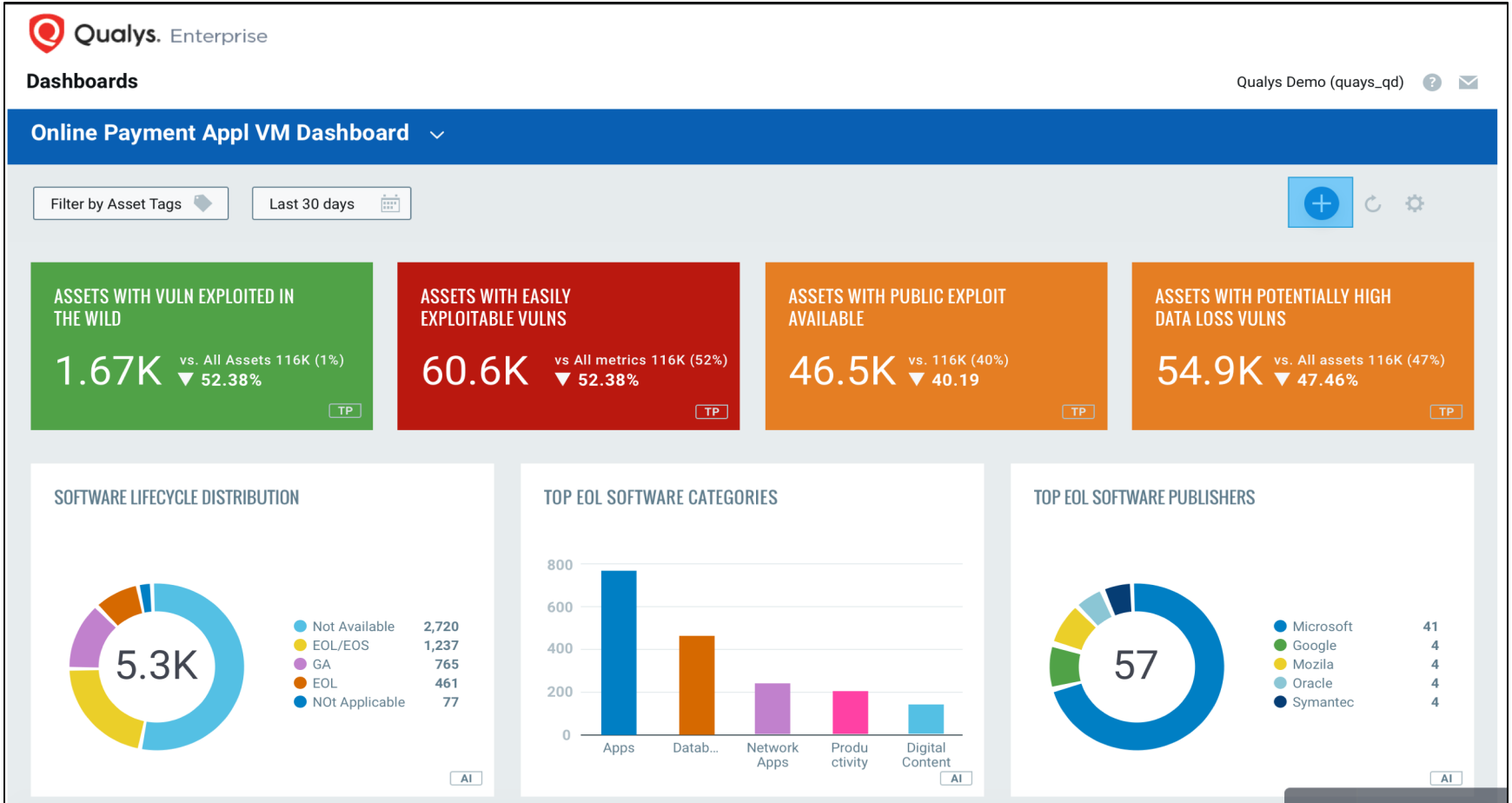
What applications are running on it?

DEMO

Dashboards

Dashboard Tool Box

Qualys Unified Dashboard



Unified Dashboard

Build dashboards with widgets from multiple Qualys Cloud Apps

Target servers, containers, instances, web apps, etc. using Asset Tags

UD

PREVIEW

Unified Dashboard

Unified Dashboard Rollout

Phase 1 – Q3 2019

Unified Dashboard App

Global dashboard filters

Support for:

VM PC FIM IOC

AI PM CRI TP

Phase 2 – Q1 2020

Unified widget builder

Upgrade existing Cloud App Dashboards

Support for:

WAS WAF SAQ

CS CV

Qualys.

Thank You

Felix Jimenez
fjimenez@qualys.com

Qualys Security Conference
Mumbai, India

सुस्वागतम

Qualys.